TSID가 활성화된 경우 FMC에서 Cisco Smart Licensing 트래픽을 toos.cisco.com으로 보고

목차

문제

FMC(Firepower Management Center) 및 FTD(Firepower Threat Defense)는 Cisco Smart Licensing HTTPS 트래픽을 `tools.cisco.com`이 아닌 `toos.cisco.com`으로 보고합니다.
이로 인해 Cisco 디바이스 라이센싱 트래픽(ASA, 라우터, 스위치)이 URL 기반 또는 보안 인텔리전스 정책에 의해 차단되어 라이센스 만료가 발생할 수 있습니다.

트래픽 자체는 합법적이며 Cisco 라이센싱 인프라로 전달됩니다.

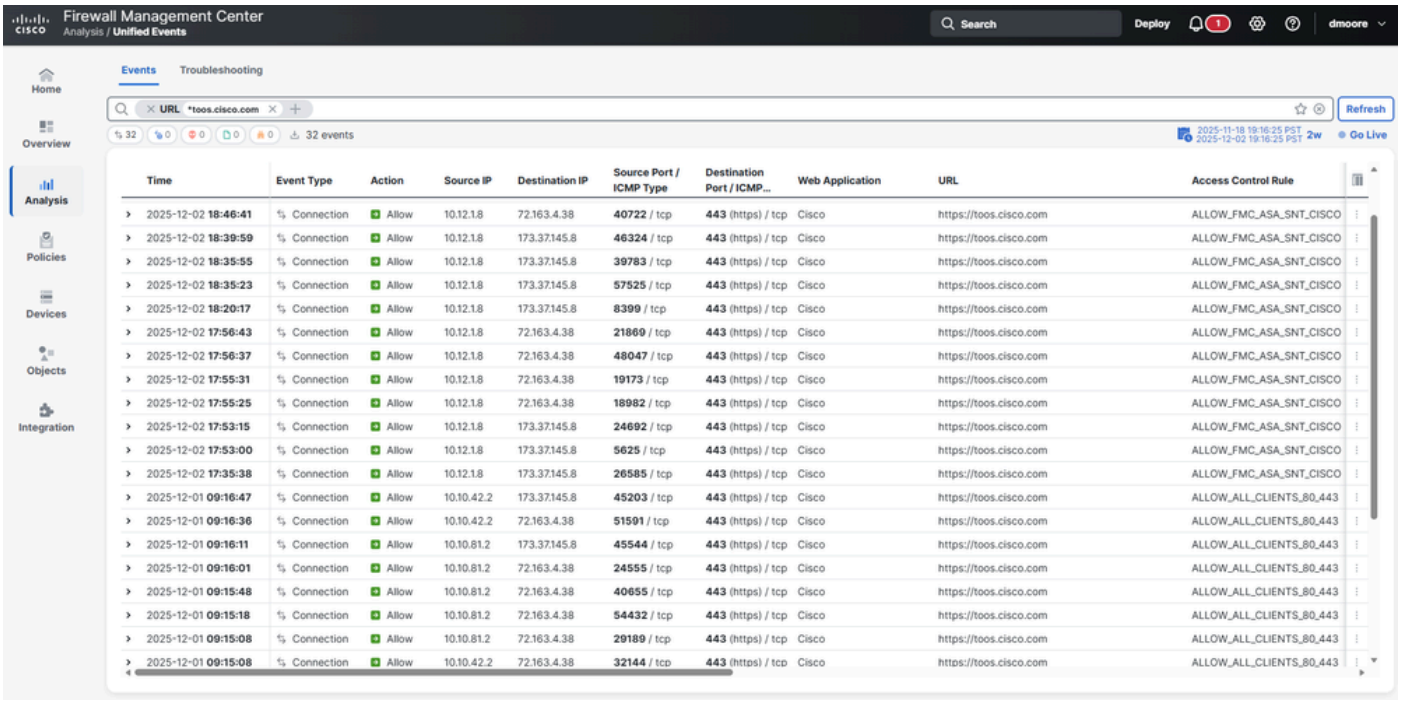
환경

- 제품군: Cisco 보안 방화벽
- 트래픽 유형: Cisco Smart Licensing(HTTPS/TCP 443)
- TSID(TLS 서버 ID) 기능 사용

해결

증상

- FMC 연결 이벤트 또는 FTD 시스템 지원 추적 표시:



- Smart Licensing 명령(예: `license smart renew auth`)이 실패합니다.
- URL 필터링/보안 인텔리전스 정책 차단 `toos.cisco.com`.
- 패킷 캡처는 트래픽이 Cisco 라이센싱 IP(예: `tools1.cisco.com`)로 전송되는지 확인합니다.
- TSID를 비활성화하면 FMC에서 tools.`cisco.com`을 보고합니다.

문제 해결/조사 단계

Smart Licensing 트래픽 확인

Cisco 디바이스(예: ASA):

```
license smart renew auth
```

Cisco 디바이스에서 트래픽 캡처(ASA 예)

```
capture LIC interface outside trace detail match tcp host <ASA_IP> any eq 443
show capture LIC
```

캡처를 내보내고 대상 IP가 Cisco 라이센싱 호스트로 확인되는지 확인합니다.

```
tools1.cisco.com
```

FTD에서 트래픽 캡처 또는 추적

패킷 캡처(FTD CLI)

```
capture capin interface <inside> match tcp host <DEVICE_IP> any eq 443
capture capout interface <outside> match tcp host <DEVICE_IP> any eq 443
```

시스템 지원 추적

```
system support trace
```

다음과 유사한 로그 항목을 찾습니다.

```
url toos.cisco.com
```

FMC에서 TSID 컨피그레이션 확인

- Access Control Policy로 이동합니다.
- 해당 규칙 수정
- 고급 설정 확인
- TLS TSID(Server Identity Discovery)가 활성화되었는지 확인

TSID 영향 검증(선택적 테스트)

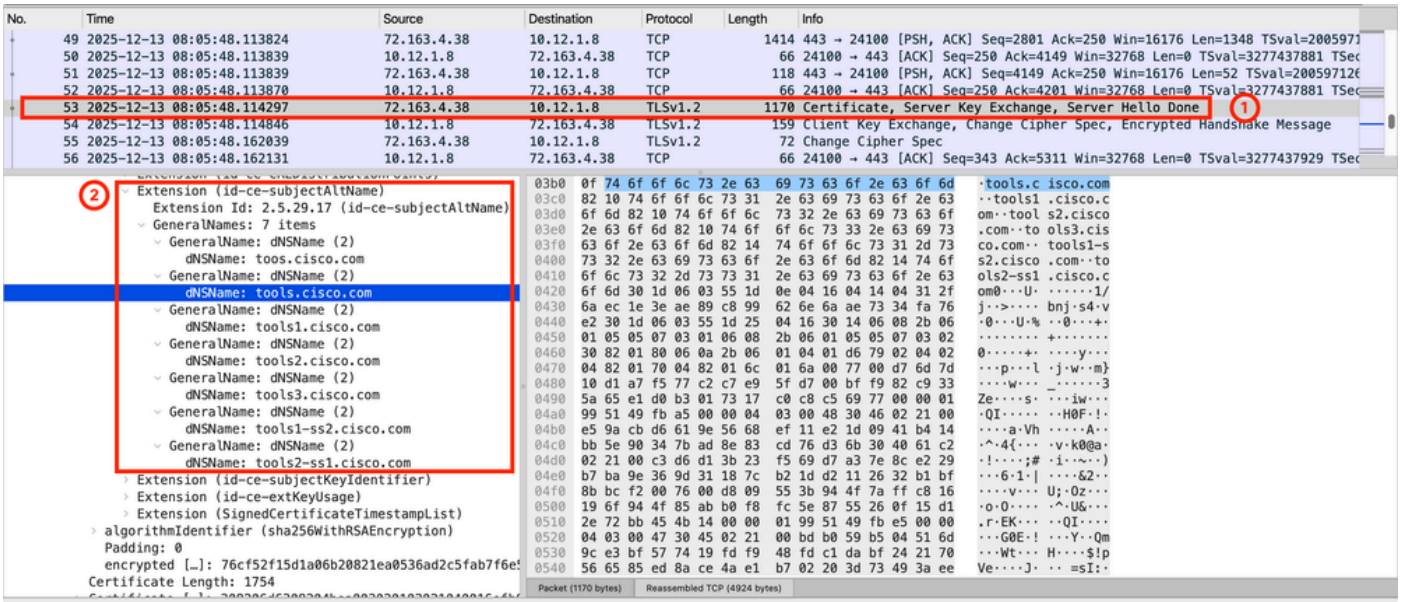
- 규칙에서 TSID 비활성화
- 정책 구축
- 라이선스 다시 실행 시도

참고 - 필요한 동작: TSID가 비활성화된 경우 FMC에서 tools.cisco.com을 보고합니다.

Inspect Server Certificate(선택 사항)

패킷 캡처 또는 브라우저 툴에서 다음을 확인합니다.

- SAN 목록에는 첫 번째 항목으로 toos.cisco.com이 포함되어 있습니다.



해결/권장 처리

결함은 없습니다. 행동은 설계에 의한 것이다. 다음 옵션 중 하나를 알려주십시오.

1.- URL 필터링/보안 인텔리전스 정책에서 toos.cisco.com 허용

2.- 다음을 통해 Cisco Smart Licensing 트래픽을 허용합니다. URL 카테고리 또는 더 광범위한 도메인 패턴

원인

TLS ClientHello에 SNI가 포함되어 있지 않은 경우 TSID 동작이 설계되어 있습니다.

TSID가 활성화되어 있고 SNI가 없는 경우 FMC는 다음 순서로 인증서 특성을 사용하여 서버 ID를 확인합니다.

1.- 공통 이름(CN)

2.- 첫 번째 주체 대체 이름(SAN)

3.- 조직 구성 단위(OU)

Cisco Smart Licensing 서버 인증서에는 첫 번째 SAN 항목으로 `tоos.cisco.com`이 포함됩니다. 따라서 FMC는 다음과 같은 경우에도 `tоos.cisco.com`을 보고합니다.

- DNS 확인이 정확함
- 대상 IP가 Cisco 라이센싱 인프라에 속함
- 트래픽 무결성은 영향을 받지 않음

이는 URL 보고 및 정책 시행에만 영향을 줍니다.

관련 콘텐츠

- TLS 서버 ID 검색

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.